GrapheneOS

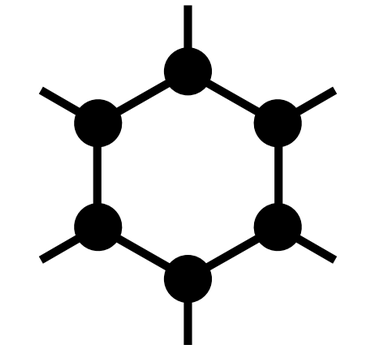
최근 수정 시각: 2026-08-19 12:32:31

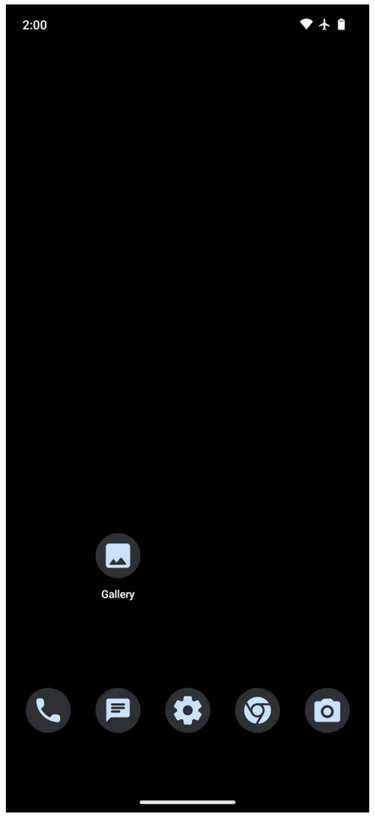
분류:Android/파생 | 2019년 출시 | 프라이버시

📱 모바일 운영체제
[펼치기 · 접기]

목차

1. 개요
2. 역사
3. 보안 철학
4. 특징
5. 지원 기기
6. 설치 및 배포
7. 제한점
8. 수용
9. 기능
10. 기타
11. 관련 문서





개발자	GrapheneOS Foundation
기반	Android
출시	2019년 4월
개발 언어	C, C++, Java, Kotlin, Rust
플랫폼	Arm
커널	Linux(linux-hardened)
커널 종류	단일형 커널
홈페이지	

1. 개요

GrapheneOS Foundation에서 개발하는 보안과 프라이버시 강화를 목표로 개발된 AOSP 기반의 모바일 운영 체제. CopperheadOS의 정신적 후속작이다.

2. 역사

GrapheneOS는 원래 CopperheadOS의 공동 개발자였던 Daniel Micay가 2019년 이후 단독으로 개발을 이어가면서 시작되었다. CopperheadOS가 상업적 노선으로 전환된 이후, GrapheneOS는 비영리 프로젝트로서 보안 연구자 중심 커뮤니티와 함께 발전하고 있다. 2020년대 들어 Google Pixel 시리즈에 맞추어 정식 지원을 확립하며 대중적 인지도를 확보하였다.

2025년 8월, 구글이 개발자 인증을 강제하는 정책을 2026년 9월부터 시행할 예정에 따라 이에 반발한 사용자들의 대체제로 다시 주목받고 있다.

3. 보안 철학

GrapheneOS는 "보안을 최우선으로, 프라이버시는 그 위에 구축된다"는 철학을 기반으로 설계된다. 기본 운영체제의 취약점 완화와 격리 강화를 우선시하며, 이를 통해 루팅, 포렌식, 원격 공격에 대한 저항성을 높인다. 그 위에 선택적으로 프라이버시 강화 기능을 제공하여 사용자가 균형 잡힌 환경을 구성할 수 있도록 한다.

4. 특징

안드로이드의 기본 구조를 유지하면서도, 취약점 완화와 격리 강화, 권한 제어 확장 등을 통해 상용 안드로이드보다 독보적으로 높은 수준의 보안성을 제공하며 현재까지도 해킹할 수 없는 애플의 락다운 모드보다도 뛰어난지라 현재 알려진 것들로는 사실상 해킹이 불가능한 OS 중 하나다. 앱의 접근 권한 자체를 격리 시킬 정도.

시스템 전반에 취약점 완화 및 프라이버시 강화 패치가 적용되어 해킹이나 디지털 포렌식 등 외부 침입 시도를 효과적으로 차단한다. 또한, 격리된 Google Play 환경을 제공하여 보안과 프라이버시를 유지하면서도 플레이 스토어 등 주요 서비스를 이용할 수 있다.

WebUSB를 통한 설치를 지원하여 다른 커스텀 펌웨어보다 설치가 간편하며, 오픈 소스 친화적인 Google Pixel 전용으로 개발되어 버그 발생이 적고 순정 펌웨어에 가까운 안정성과 완성도를 제공한다.

5. 지원 기기

GrapheneOS는 Google Pixel 시리즈만을 정식 지원한다. 픽셀 기기는 오픈 소스 친화적일 뿐 아니라 ARM MTE와 같은 최신 보안 기술을 선도적으로 도입하여 보안 강화에 적합한 환경을 제공한다. 또한 특정 기기군만을 지원함으로써 다양한 기기를 포괄할 때 발생할 수 있는 코드베이스의 복잡성과 잠재적 취약점을 줄일 수 있다.

기기마다 지원 기간이 천차만별인 타 커스텀 펌웨어와는 달리, GrapheneOS는 구글의 Google Pixel 지원 정책을 따라가므로 Pixel 제품 구매 시 반드시 구매하려는 기기의 지원 기간을 필히 확인해야 한다.

정식 지원 기종은 Google Pixel 6 이후 모델이며, Google Pixel 4a 5G 이후 모델은 연장 지원 대상에 포함된다. 단, 연장 지원 기기는 구글의 공식 보안 업데이트가 종료된 상태이므로 장기적인 사용이나 신규 구입은 권장되지 않는다. 가능하다면 ARM MTE를 지원하는 Pixel 8 이후 기기를 사용하는 것이 권장된다. 또한 Pixel 6 이후 기기에서는 Titan 보안 프로세서를 활용하여 브루트 포스 공격을 효과적으로 방어할 수 있다.

2025년 10월 13일, Google 측의 느린 보안 업데이트에 불만을 가진 것을 계기로 주요 Android 제조사와 협력해 2026년부터 퀄컴 스냅드래곤 AP를 탑재한 기기에 GrapheneOS를 공식 지원할 것이라는 소식이 있다.# 또한 기존 Google Pixel 지원의 경우 이 결정으로 인해 추후 지원 계획이 불투명해졌다.

이후 2026년 3월 2일 발표를 통해 앞서 언급된 Android 제조사의 정체는 모토로라 모빌리티로 밝혀졌다.#

6. 설치 및 배포

GrapheneOS는 WebUSB 기반의 공식 설치 도구# 를 제공하여 사용자가 브라우저를 통해 손쉽게 기기에 설치할 수 있다. 설치 과정에서는 부트로더 언락이 필요하며, 설치 후 Verified Boot 체인을 통해 운영체제의 무결성이 검증된다. Pixel 6 이상의 기기에서는 부팅 시 표시되는 Verified Boot 키 해시값을 GrapheneOS 공식 웹사이트# 에 게시된 해시값과 비교하여 펌웨어 변조 여부를 확인할 수 있다. 공식적으로는 OTA 업데이트를 제공하여 장기간 안정적으로 유지할 수 있다.

7. 제한점

GrapheneOS는 오직 Google Pixel 기기만 지원하기 때문에 기기 선택의 폭이 제한된다. 또한, 구글 서비스는 기본적으로 포함되지 않으며 Sandboxed Google Play를 별도로 활성화해야 한다. 또한 활성화되지 않을 경우 Aurora Store를 통해 일부 앱을 설치할 경우 구글 알림 서비스에 의존하는 앱이 제대로 작동되지 않을 수 있다.

커스텀 롬이기 때문에 일부 은행·결제·스트리밍 앱 등은 보안 검증(Play Integrity API, SafetyNet 등)이나 DRM 사용의 제약으로 동작하지 않을 수 있다.

8. 수용

GrapheneOS는 보안 연구자들과 프라이버시 지향 사용자들 사이에서 높은 평가를 받고 있으며, 에드워드 스노든 역시 공개적으로 사용을 권장한 바 있다. 언론에서는 "일반 사용자가 접근할 수 있는 가장 안전한 모바일 운영체제"로 평가되기도 한다. 다만 제한된 기기 지원과 구글 서비스 의존성 문제는 대중적 확산의 걸림돌로 지적된다.

9. 기능

GrapheneOS는 다양한 보안 및 프라이버시 기능을 제공한다.

- Sandboxed Google Play
  구글 플레이 서비스를 샌드박스 환경에서 실행하여 시스템 전역 침범을 막으면서, 구글 플레이 스토어, 구글 플레이 게임 등 관련 서비스를 안전하게 이용할 수 있도록 지원한다.

- Vanadium
  GrapheneOS 팀이 개발한 보안 강화 브라우저로, Spectre 공격 벡터로 악용될 수 있는 JavaScript JIT와 WebAssembly 등을 차단하고 강력한 안티 핑거프린팅을 제공한다. Chromium 기반으로 제작되었으나, 구글 관련 구성 요소는 모두 제거되었다. 또한 GrapheneOS의 모든 앱에서 사용하는 WebView는 Vanadium을 통해 동작한다.

- AOSP보다 향상된 권한 관리
  네트워크·센서 등 기본 AOSP에서는 제어할 수 없는 권한까지 관리할 수 있으며, Storage Scopes 기능을 통해 iOS와 유사하게 특정 파일만 앱에 접근 허용이 가능하다.

- USB 포트 보호
  잠금화면 상태 등 특정 조건에서 USB 연결을 차단하여 디지털 포렌식 장비 접속이나 USB 포트를 통한 글리칭 공격을 방지한다. 이는 애플의 락다운 모드와 유사한 기능이다.

- 자동 재부팅
  AFU(After First Unlock) 상태가 장시간 지속될 경우 기기를 자동으로 재부팅하여 메모리에 남아 있는 복호화 키를 제거하고 포렌식을 방지한다. 재부팅까지의 대기 시간은 사용자가 직접 설정할 수 있으며, 잠금 해제 시 타이머는 초기화된다. BFU(Before First Unlock) 상태에서는 자동 재부팅이 동작하지 않는다.

- 하드웨어 암호화 키 격리
  Google Pixel 6부터 탑재된 Titan M2 보안 프로세서를 활용해 사용자 PIN/비밀번호와 하드웨어 키를 결합, 암호화 키를 보호한다. 또한 하드웨어 수준에서 암호 입력 지연을 적용해 브루트 포스 공격 시 시도 간격을 기하급수적으로 늘려 데이터를 보호한다.

- Duress PIN/Password
  실제 복호화 암호가 아닌 별도의 가짜 암호를 설정해, 강제로 암호 제공을 요구받을 경우 입력 시 기기 데이터를 초기화하고 eSIM을 포함한 모든 민감 정보를 삭제할 수 있다. 이는 잠금화면뿐 아니라 시스템 전반의 암호 입력 창에서도 작동한다.

- 구형 셀룰러 기술 및 5G 차단
  2G[1], 3G[2] 등 공격 벡터로 악용될 수 있는 구형 통신 기술과 보안 문제가 제기되는 5G를 차단하는 LTE Only 모드를 제공한다.

- 강화된 Linux 커널
  linux-hardened 커널을 기반으로 각종 취약점을 완화한 보안 패치가 적용되어 있다.

- 강화된 malloc 및 libc
  hardened_malloc와 수정된 C 표준 라이브러리를 사용해 메모리 관련 취약점을 완화한다.

- 강화된 샌드박싱
  SELinux와 BPF 정책을 보강하여 AOSP보다 강력한 샌드박싱을 제공하며, 네이티브 코드 디버깅 등 샌드박스를 약화시킬 수 있는 기능을 차단한다.

- ARM MTE 강제 적용
  ARM MTE(Memory Tagging Extension)를 특정 앱 또는 모든 앱에 강제 적용하여 버퍼 오버플로우 등 메모리 안전 취약점을 하드웨어 수준에서 차단한다. Google Pixel 8 이후 기종에서만 사용 가능하다.

- 안전한 앱 스포닝

Zygote 대신 exec 방식을 사용해 앱을 실행함으로써 더 빠르고 안전한 앱 스포닝을 제공한다. 다만 일부 게임 등에서는 호환성 문제가 발생할 수 있다.

- 더 많은 유저 프로필 제공
  샌드박싱된 유저 프로필을 게스트를 포함하여 최대 32개 제공하여 여러 용도에 따라 각 앱들을 따로 격리된 환경에서 사용이 가능하다.

- VoLTE 지원
  별도의 패치 없이 한국, 중국 등의 국가에서 VoLTE를 활성화할 수 있다. #

- 통화 녹음
  다이얼 앱에서 통화 녹음을 지원한다. # 다만 삼성 갤럭시, 에이닷, 익시오의 통화 녹음과 다르게 자동 녹음 기능이 없어서 통화할때 마다 녹음 버튼을 따로 눌러줘야 한다.

- 카메라 셔터음 제한
  카메라 셔터음이 강제되는 지역에서 셔터음을 제거할 수 있다. #

10. 기타

GrapheneOS는 상술한 다양한 취약점 완화 패치 및 수정으로 인해 일부 앱[3]에서 심각한 버그나 작동이 불가능할 수 있다. 이 경우, 취약점 완화 기능을 끄면서 타협하거나 사용하지 않는 것이 좋다.
각국의 금융앱 호환은 해당 웹페이지를 참고하여 확인할 수 있다. GrapheneOS 공식과는 별개의 사이트이다. 금융앱이 절대 호환되지 않는다는 말은 잘못된 이야기이며, 심지어는 상기된 GrapheneOS의 강력한 권한제어를 통해 V3 Mobile Plus 앱의 네트워크 권한을 차단하여 사용해도 V3앱의 알림 권한만 잘 준다면 금융 앱 자체는 멀쩡히 동작한다.[4] 또한 SafetyNet은 호환이 안되는 관계로 이를 사용하는 모든 앱들은 실행이 불가능하다.

프라이버시를 위해서는 카카오톡, 네이버 등의 대한민국 정부 기관에 정보를 제공하는 기업의 앱 및 정부에서 개발한 앱은 설치하지 않는 것이 좋다. 사용을 피할 수 없다면 프라이빗 스페이스[5]를 열어서 그곳에 앱을 설치하는 식으로 격리를 해줄 수 있다. 그러나 어지간해서는 별도의 기기를 마련해서 사용하자.[6]

스페인 카탈루냐의 마약 범죄 조직이 해당 운영체제를 이용해 활동하는 정황이 포착되었다. # 이에 GrapheneOS측은 부정적인 여론이 확산되는 것을 우려했는지 공식 X를 통해 "유럽의 권위주의자들과 그들을 돕는 언론들은 GrapheneOS와 심지어 픽셀 폰까지도 마치 범죄자들을 위한 것인 양 잘못 묘사하고 있다. GrapheneOS는 이 사람들이 모든 사람에게 강요하려는 대규모 감시 경찰 국가에 대해 반대한다"라는 성명문을 게시하였다.

GrapheneOS의 카메라 앱은 GitHub을 통해 APK 파일을 공식 배포하고 있다. #

순정의 경우 한글 키보드를 지원하지 않는다. 한글을 사용하려면 별도의 키보드 앱 설치가 필요하다.

공식 커뮤니티의 경우 대체로 엄격한 편으로, 특히 GrapheneOS 팀은 소셜 미디어에 적극적으로 상주하며 직설적인 말투로 가짜 정보 및 루머를 바로잡는데 매우 적극적인 편이다. 다만 종종 직설적인 것을 넘어 공격적으로 대응하고 배타적인 성향이 강하다보니 Toxic하다는 얘기도 듣는다.

11. 관련 문서

- /e/OS: 이쪽도 탈구글화 및 개인정보 보호에 최적화되어 있는 커스텀 펌웨어다.
- Google Pixel
- 모토로라 모빌리티

CC BY NC SA

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.